

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-298088

(43)Date of publication of application : 11.10.2002

(51)Int.Cl.

G06K 17/00
G06F 17/30
G06F 17/60
G09C 1/00
H04L 9/08
H04L 9/32
// B42D 15/10

(21)Application number : 2001-101088

(22)Date of filing : 30.03.2001

(71)Applicant : BALTIMORE TECHNOLOGIES JAPAN CO LTD

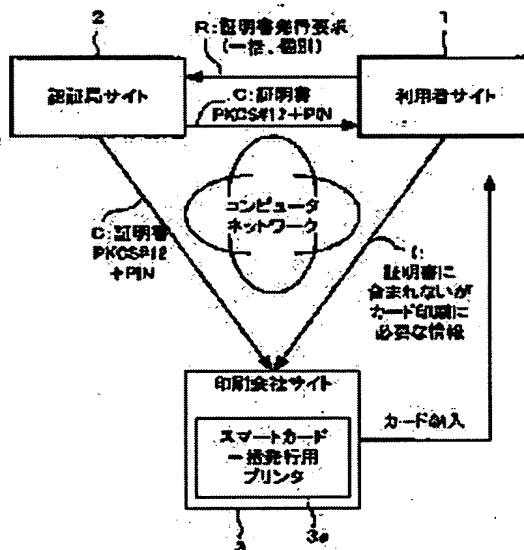
(72)Inventor : SAKURAI KEITA
JANE GREENHOUSE PIRO
ASANO MASAKAZU
SHIBAZAKI TADAO

(54) SMART CARD ISSUE SYSTEM AND METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a secure and smart card issue system capable of issuing a card relatively simply.

SOLUTION: This smart card issue system is provided with a user's site using the smart card, an identification department's site issuing a certificate by a demand of the user's site, and a printing site receiving the certificate from the identification department's site, receiving a peculiar information to be printed on a card from the user's site, and producing the smart card. The user's site, the identification department's site and the printing site are connected by a computer network and can mutually communicate data. The user's site is provided with a means collectively or individually demanding the issue of the certificate to the identification department's site, and a means transmitting the peculiar information to be printed on the card to the printing company's site when collectively issuing the smart cards.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

(3)

一括して鍵を作成するとともにデジタル証明書を発行するステップと、
前記デジタル証明書を送信するステップと、
カードの固有情報を取得するステップと、
前記デジタル証明書及び前記固有情報に基づき一括してカードを発行するステップと、

【発明が解決しようとする課題】スマートカードは例え

前記人事データベース内の対象者に対して個別にカードの発行を要求するステップと、
個別に鍵を作成するとともにデジタル証明書を発行するステップと、
前記デジタル証明書に基づき個別にカードを発行するステップと、を備えるスマートカード発行方法。
【発明の詳細な説明】
[0001]
【発明の属する技術分野】この発明は、ＩＣカードなどのスマートカード発行に用いられるスマートカード発行システム及び方法に関する。

(b) (7)(C), (b) (7)(D).

【従来の技術】従来、社員スタレジットの分野で磁気カードが広く使われていた。しかし、機能及び安全性の観点からICカードへの移行が進みつつある。今後、ICカードは、オンラインショッピングやネット取引に

【発明の要旨】従来、社員スタレジットの分野で磁気カードが広く使われていた。しかし、機能及び安全性の観点からICカードへの移行が進みつつある。今後、ICカードは、オンラインショッピングやネット取引に

【0008】

【課題を解決するための手段】この発明に係るスマートカード発行システムは、スマートカードを利用する利用者に、スマートカードの発行に必要とする事項を確認させることにより、本人であることを確認することによって、本人による不正な利用を防ぐことを可能にする。

【0003】このための技術がデジタル証明書である。デジタル証明書は、インターネット上で電子商取引を行う際の暗号化プログラム「秘密かぎ」(公開かぎ)のうち、公開かぎの所有者を特定するものである。デジタル証明書(以下、単に「証明書」と記す)、ICカードなどのスマートカードに搭載されて暗号証に用いられている。今後、証明書へのニーズは高まると予想されている。

【0004】秘密かぎや証明書はパソコン内に搭載されることが多く、第三者によるパソコンの不正利用を完全には防げなかった。これに対して、秘密かぎと証明書を、スマートカードに搭載する、不正利用を防げるうえ、利用環境も広がる。さらに、非接触のICカードと組み合わせて使うことにより、すなわち1枚のカード上に接触(Public-Key Infrastructure (PKI)用)と非接触用(Chip)を搭載した総合カードとすることにより、カード一枚で入退室管理や社員食堂の決済などさまざまな場面に対応できる利点もある。

【0005】PKIをICカードに格納することにより、次のようなメリットが得られる。・PC上にファイルとしてある場合は、ソフトがコピーされる危険があるが、ICカードに格納されればICカードの中から秘密鍵を不正にコピーしたり、ICチップの内部にアクセスすることは限りなく不可能になる。すなわち耐タンパ性に優れてい

証明書を受けるとともに、前記個別発行処理部の検索結果を受けてスマートカードを印刷するカード少量発行用プリンタとを備える。

【0010】好ましくは、前記利用者サイトは、利用者の個人情報が記憶されている人事データベースと、前記人事データベースから所定の条件に基づき人事データを抽出してスマートフォンカードの発行リストを作成する発行リスト作成部と、前記発行リストに基づき前記認証局サイトに対して鍵及び証明書生成を要するカード一括発行要求部と、前記認証局サイトから印刷に必要な情報の要求を受けたとき、当該情報を送信するカード固有情報送信部と、前記人事データベースから所定の条件に基づき人事データを抽出して個別にスマートフォンカードを発行する発行部とを備える。

【0011】好ましくは、さらに、少なくとも有効期限が切れた又は利用者の同意の場合にその利用者の証明書書の失効を前記認証局サイトに要求するカード失効要求部と、発行済みの所定の証明書書を選択し、鍵ペアと証明書とを格納する前記認証局サイトに要求する鍵ペアと、前記認証局の鍵のリカバリを要求する鍵リカバリ要求部と、前記認証局に対して過去のログの閲覧を要求するログ閲覧部とを備える。

【0012】好ましくは、前記認証局サイトは、鍵を生成し、証明書要求・発行の管理を行うとともに、鍵アーカイブを行うサーバと、前記鍵、前記証明書の要求・発行、ログのデータを格納するデータベースと、前記利用者サイトの設定情報を管理するレジストリと、前記利用者サイト及び前記印刷会社サイトに送受信を行う送受信部とを備える。

【0013】この発明に係るスマートカード発行方法は、スマートカードの発行リストを作成するステップ

と、前記発行リストに基づきカードの一搭発行を要求するステップと、一括して鍵を作成するとともにデジタル証明書を送付するステップと、前記デジタル証明書を送付するステップと、カードの固有情報を受取るステップと、前記デジタル証明書及び前記固有情報に基づき一括してカードを発行するステップと、前記発行リストの一部について個別にスマートカードを発行すべき者を指定するステップと、前記指定に基づきカードの個別発行を要求するステップと、個別に鍵を作成するとともにデジタル証明書を送付するステップと、前記デジタル証明書と、前記カードを発行するステップと、を備えるものであ

る。【0014】この発明に係るスマートカード発行方法は、所定の条件に従い、前記データベースを検索して発行に対象者を抽出するステップと、抽出された発行対象者に対してカードの一元発行を要求するステップと、一括して鍵を作成するとともにデジタル証明書を作成するステップと、前記デジタル証明書を送信するステップと、カードの固有情報を取得するステップと、前記デジタル証明書及び前記固有情報に基づき一括してカードを発行するステップと、前記人事データベース内の対象者に対して個別にカードの発行を要求するステップと、個別に鍵を作成するとともにデジタル証明書を作成するステップと、前記デジタル証明書を取得するステップと、前記デジタル証明書に基づき個別にカードを発行するステップと、を備えるものである。

【0015】この発明は、スマートカードの大規模発行を行いたい場合に用いられるシステムに関するものである。本システムは、スマートカードへ証明書を大規模に発行するプロセスを実行するものであり、証明局情報サイトや、カード種類、印刷会社、発行プロセスに必要なインフラ選定など、いくつものオプションを選択するだけで、スマートカード発行用の証明局を構築することができ

[0016]

【発明の実施の形態】この発明の実施の形態に係るシステム/方法について図面を参照して説明する。図1は、この発明の実施の形態に係るシステムの全体構成を示す図である。このシステムは、スマートフォンを発行・利用する企業などが管理運営する利用者サイト1と、利用者サイト1の要求により証書を発行する認証局サイト2と、スマートフォンを印刷・生産する印刷会社サイト3とを描える。これら3つのサイトの間にはコンピュータネットワークで接続されており、相互にデータ通信可能である。

【0017】利用者サイト1はスマートカードの発行を要求するサイトである。発行されたスマートカードは、例えば出込郵便管理、入退勤管理、アクセスコントロール、S/MIMEメール、決済システムなどに利用される。利用者サイト1は、認証局に対して一括あるいは個別に証明発行を要求す機能と、一括にスマートカードを発行するときに印刷会社サイト3に対してカードに印刷する固有情報を送信す機能を備える。また、利用者サイト1は、証明片一括送付、個別失効を含む証明書ライフサイクル管理機能を備える。

【0018】印刷会社サイト3は、証明書及びカードに印刷する固有情報を受信してスマートカードを印刷するとともに、完成したカードを配送する機能を備える。印刷会社サイト3では、発行枚数や期間などにより最適な印刷ラインが案件ごとにより構築される。発行枚数が多い場合は、同時に複数の印刷ラインが稼働して短期に合

わけてパフォーマンスを提供可能である。

【0019】 認証局サイト2は、利用者サイト1から証明書発行要求を受け、鍵を生成して証明書を発行するとともに、鍵、証明書をデータベースに記憶して保存する。認証局サイト2はPKCS#12とPINを送信する。PKCSは公開鍵暗号標準 (Public Key Cryptography Standard) である。PINはPersonal Identification Numberの略であり、PKCS#12ファイルは複合するためのIDのことである。なお、使用可能な形式はPKCS#12に限定されない。現在の他の形式あるいは将来採用される形式を用いることができる。また、送信データに識別IDや、その他の付随情報も含めるようにしてもよい。

【0020】 図2は、利用者サイト1の内部構成を示す図である。人事データベース11には、利用者である企業などの社員・会員の人事情報、例えば、氏名、性別、生年月日、所属、役職などが記憶されている。発行リスト作成部12はスマートカードを発行するリストファイルを作成する。発行リスト作成部12は、例えば、新入社員の人件データを抽出して新入社員用カード発行リストファイルを作成する。この際、所属情報に基づき入退社可能なエリアの情報を付加することもできる。このシステムはCSV、LDP形式のリストファイルによる申請情報のインポート機能を提供する。ファイル項目として、識別ID、DNリソースが含まれる。なお、発行リスト作成部12を、図示しない人事データベースシステム等との接続により、なお、データベースを用いて社員リストなどのソースから手作業に発行リストを作成してもよい。

【0021】 発行リスト作成部12の出力を基に、審査あるいは自動による審査を行った後、発行リスト13が確定し、メモリに記憶される。カード一括発行要求部14は、発行リスト12に基づき認証局サイト2に対して証明書・鍵の生成を一括して要求する。カード固有情報送信部15は、印刷会社サイト3から印刷に必要な情報の要求を受けたとき、当該情報を送信する。例えば、識別IDに対応する氏名、性別、生年月日、所属、役職などを送信する。

【0022】 以上印刷会社サイト3に一括してスマートカードの発行を要求するためのものである。本システムはスマートカードを個別に発行することもできる。個別発行処理部16は、人事データベース11から個別にスマートカードを発行すべき社員を検索する。例えば、途中入社、人事異動に該当する社員を検索する。紛失の際はスマートカードの再発行を手動で行うこともできる。あるいは、個別発行処理部16はすでに作成された発行リストから選択した、手入力したりして個別発行するリストを作成する。カード少量発行要求部17は、認証局サイト2に対してカード少量発行時の鍵生成・証明書を要求するとともに、認証局サイト2から証明書を取得する。スマートカード少量発行用プリンタ18は、

【0029】 図4は、システム全体の動作フローチャートである。ステップS1～S10は一括発行要求の処理の流れを示す。

S1：人事データベース11から証明書発行対象者を抽出する。年度始めの異動対象者を抽出したり、新入社員を抽出したりする。

S2：所定の審査を行った後、発行リスト13を作成し、認証局サイト2へ一括して証明書の発行要求を発行する。

S3：認証局サイト2は、要求を受けて鍵生成を行い、証明書を発行する。

S4：発行されたPKCS#12とPINをカード印刷会社3へキューに配送される。送信プロトコルはhttpsを用い、取得情報はクライアント側データベースに暗号化されて格納される。

【0030】 S5：証明書は鍵アーカイブ（データベース23）に記憶される。

S6：印刷会社サイト3はカード印刷のための情報を利用者サイト1に要求する。

S7：利用者サイト1からカード固有の情報を受信する。

S8：ステップS4で取得した鍵ペア、PIN、証明書、及びステップS7で取得した固有の情報に基づきカードを発行（印刷）する。

S9：カードを配送する。カードの発行が完了したら、サーバ側に終了メッセージを送信し、保持していた鍵ペア、PIN、証明書を完全に削除する。

S10：利用者はカードを受領し、その運用を開始する。

【0031】 なお、ステップS7でオンラインでデータを受けていたが、これに代えてオフラインでデータやM0などの媒体で渡したり、郵便・リストなどの紙情報で渡してもよい。

【0032】 ステップS1～S10は一括発行要求の処理の流れを示す。

S11：認証局サイト2に対して個別に証明書発行を要求する。例えば、途中入社、人事異動、退職などの場合である。個別発行処理部16でGUILによる申請あるいはCSV形式のリストファイル入力を行い、その要求を認証局サイト2へ送る。

S12：認証局サイト2が鍵を生成し証明書を発行する。

S13：生成した証明書PKCS#12形式、PINを利用者サイト1へ送る。

S14：取得した証明書をポータブルカードプリンタ18にてスマートカードに格納する。なお、ポータブルプリンタ18において、スマートカード内で鍵生成を行い、認証局サイト2へ証明書要求を出すようにしてもよい。

【0033】 本発明は、以上の実施の形態に限定される

ことなく、特許請求の範囲に記載された発明の範囲内、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。

【0034】 また、本明細書において、手段とは必ずしも物理的手段を意味するものではなく、各手段の機能が、ソフトウェアによって実現される場合も包含する。さらに、一つの手段の機能が、二つ以上の物理的手段により実現されても、若しくは、二つ以上の手段の機能が、一つの物理的手段により実現されてもよい。

【0035】

【発明の効果】 本システムは以下のような効果を奏する。

- ・ X. 509 証明書を格納したスマートカードを発行する場合、短期間でかつ統合的なシステムを構築することができる。

- ・ 発行リスト作成からスマートカード納品までをワンストップで提供でき、かつセキュアである。

- ・ 発行規模に応じたホスティング認証局の構築を行うことができる。

- ・ 証明書の有効期限や記載内容を自由に設定できる。

- ・ 人事データベースなどと連動したり、証明書発行リストを作成して、そのデータをもとに認証センター内で、一括での証明書発行要求を行い、認証センター内で生成した鍵ペアおよび証明書をセキュアな形で印刷会社へ送信し、その他、カード印刷に必要な情報とともにスマートカードへ印刷発行が可能である。

- ・ スマートカードを紛失した場合や、登録された場合、簡便に失効手続き (Revoke) を行うことができる。

- ・ 有効期限切れなどの場合に、大量失効手続き (Revoke Bulk Request) を簡単に実行することができる。

- ・ 生成された鍵ペアを保存する鍵アーカイブ機能を提供する。

- ・ スマートカードを破損した場合など、同一鍵ペアによるスマートカードの再発行を簡単に実行することができる。

【図面の簡単な説明】

【図1】 この発明の実施の形態に係るシステムの全体構成を示す図である。

【図2】 利用者サイト1の内部構成を示す図である。

【図3】 認証局サイト2の内部構成を示す図である。

【図4】 システム全体の動作のフローチャートである。

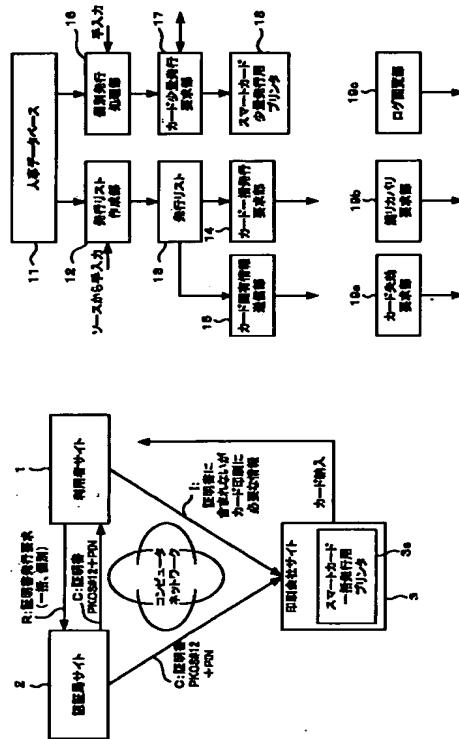
【符号の説明】

- 1 利用者サイト
- 2 認証局サイト
- 3 印刷会社サイト
- 11 人事データベース
- 12 発行リスト作成部
- 13 発行リスト
- 14 カード一括発行要求部
- 15 カード固有情報送信部

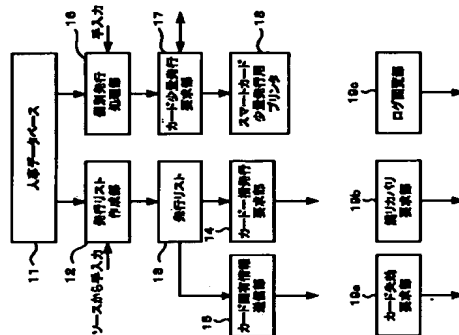
- | | |
|-----|------------------|
| 16 | 個別発行処理部 |
| 17 | カード少量発行要求部 |
| 18 | スマートカード少量発行用プリンタ |
| 19a | カード失効要求部 |
| 19b | 健りカバリ要求部 |

- | | |
|-----|-------------------|
| 19c | ログ閲覧部 |
| 21 | 送受信部 (SSL-Webサーバ) |
| 22 | サーバ |
| 23 | データベース |
| 24 | レジストリ |

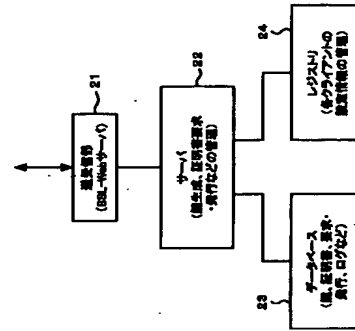
【图1】



【图2】



【图3】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	チヤーン・ド (参考)
G 0 9 C	1/00	G 0 9 C	1/00
H 0 4 L	9/08	B 4 2 D	15/10
	9/32	H 0 4 L	9/00
// B 4 2 D	15/10		6 0 1 B
			6 7 5 D

(72) 発明者	ジュエン グリーンハウス ピーロ	(72) 発明者	柴崎 忠生
	東京都千代田区紀尾井町 4-1		東京都千代田区紀尾井町 4-1
	ニューオ		ニューオ
	ータニ ガーデンコート 8 階		日本ボル
	チモアテクノロジーズ株式会社内		チモアテクノロジーズ株式会社内
(72) 発明者	浅野 昌和	F ターム (参考)	2C005 M403 M401 N402 N406
	東京都千代田区紀尾井町 4-1		5B058 K405 K411 K431
	ニューオ		5B075 N020 P005 U040
	ータニ ガーデンコート 8 階		5J104 A416 E401 E404 M401 N402
	チモアテクノロジーズ株式会社内		N435 P407